Centraal Planbureau

Kaders voor code: beleid voor veilige digitale middelen

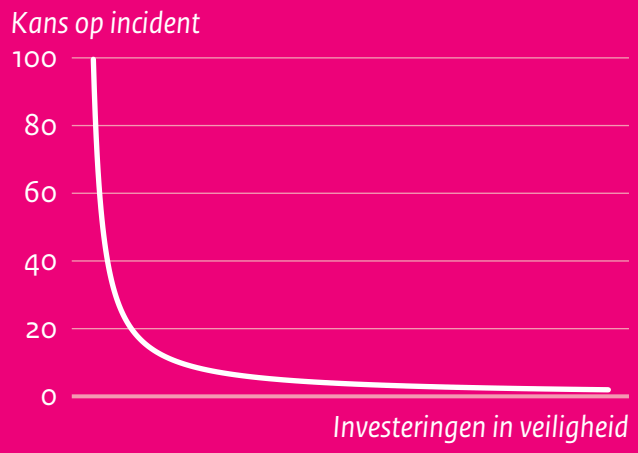
De overheid moet soms ingrijpen om digitale middelen betrouwbaarder te maken

Bij externe effecten
Als anderen worden getroffen door digitaal falen

Bij informatieproblemen
Als de consument de veiligheid van een digitaal middel niet kan beoordelen

Bij marktmacht
Als de consument moeilijk een betrouwbaar digitaal middel kan vinden

Honderd procent betrouwbaarheid is doorgaans niet haalbaar



CPB Policy Brief

Bastiaan Overvest

april 2020

Beleid voor digitale middelen

Producten en diensten digitaliseren. Dat heeft voordelen, maar digitale middelen kunnen ook onbetrouwbaar zijn.

Een digitaal product of dienst kan ondeugdelijk zijn, of niet goed beveiligd tegen aanvallen van buitenaf.
Dit kan processen verstoren, maar ook leiden tot schade aan goederen of gezondheid.

Er zijn drie redenen waarom de overheid soms moet ingrijpen

Aanbieders en gebruikers kunnen niet altijd zelf zorgen voor adequate betrouwbaarheid

Externe effecten

- Via identiteitsfraude slachtoffers in sociaal netwerk
- DDoS-aanvallen
- Ongevallen met zelfrijdende auto's

Informatieproblemen

- Consument ziet betrouwbaarheid niet
- Levert de fabrikant ná verkoop goede updates?

Marktmacht

- Fabrikanten met marktmacht stoppen te vroeg met productondersteuning
- Prijsdiscriminatie via lagere betrouwbaarheid

Mogelijke maatregelen

Aansprakelijkheid, veiligheidseisen, vooraf testen en zo nodig verbieden

Voorlichting, markt aanzetten tot transparantie en certificering

Toezicht bij fusies, markt prikkelen

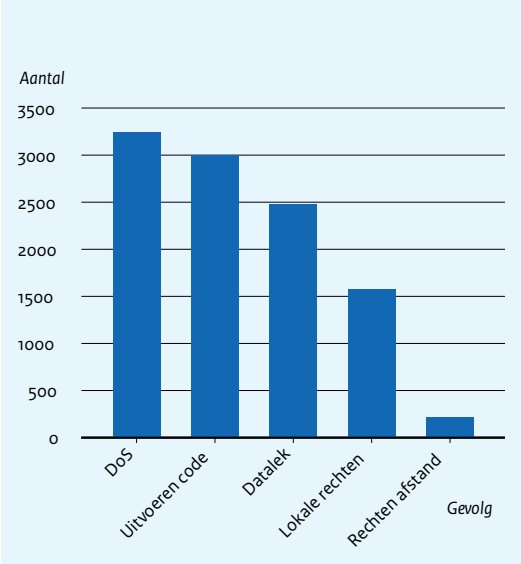
Nadelen en risico's

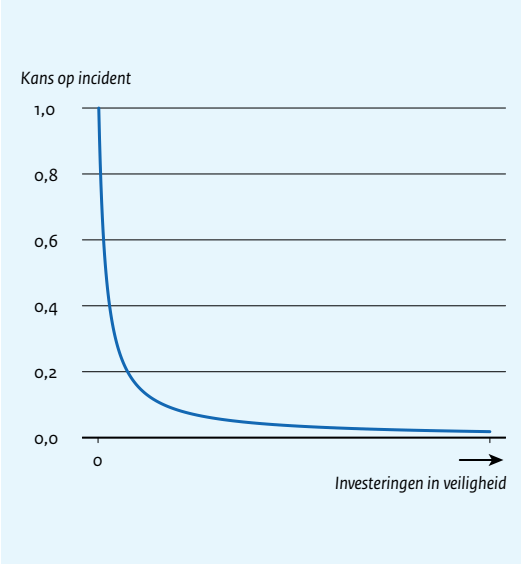
- Financiële compensatie niet voldoende bij fysieke schade.
- Risico's soms moeilijk vooraf in te schatten

Overheid doorgaans niet in een betere positie om informatie-problemen op te lossen dan marktpartijen

Verplichte ondersteunings-periode kan innovatie ontmoedigen

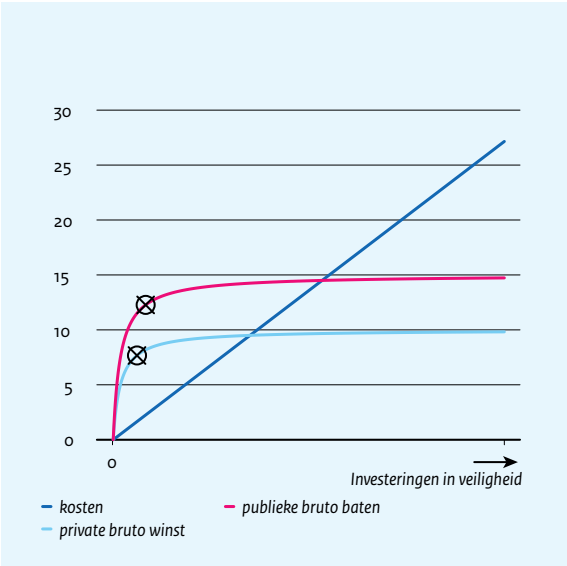
Gevolgen van bekende softwarekwetsbaarheden (links)
Kans op schade daalt als investeringen in veiligheid stijgen (rechts)





NB. De figuur links geeft voor de NCSC-adviezen uit de periode 2012 t/m augustus 2018 het gevolg van kwetsbaarheden weer die zijn beschreven in die adviezen. Gevolgen kunnen bijvoorbeeld zijn dat een kwaadwillende code kan uitvoeren ("uitvoeren code") op een computer of dat een kwaadwillende met fysieke toegang tot het apparaat beheerdersrechten kan verkrijgen ("lokale rechten"). Bron: Ruesink en Windig (2019).

Maatschappelijk optimaal investeringsniveau ligt hoger dan privaat optimaal niveau



De bolletjes geven het investeringsniveau weer waarde private en publieke netto baten maximaal zijn.

Interventieladder voor externe effecten